RFAL: Adversarial Learning for RF Transmitter Identification and Classification

Year: 2020 | Citations: 157 | Authors: Debashri Roy, Tathagata Mukherjee, M. Chatterjee, Erik Blasch, E. Pasiliao

Abstract

Recent advances in wireless technologies have led to several autonomous deployments of such networks. As nodes across distributed networks must co-exist, it is important that all transmitters and receivers are aware of their radio frequency (RF) surroundings so that they can adapt their transmission and reception parameters to best suit their needs. To this end, machine learning techniques have become popular as they can learn, analyze and predict the RF signals and associated parameters that characterize the RF environment. However, in the presence of adversaries, malicious activities such as jamming and spoofing are inevitable, making most machine learning techniques ineffective in such environments. In this paper we propose the Radio Frequency Adversarial Learning (RFAL) framework for building a robust system to identify rogue RF transmitters by designing and implementing a generative adversarial net (GAN). We hope to exploit transmitter specific “signatures” like the in-phase (I) and quadrature (Q) imbalance (i.e., the I/Q imbalance) present in all transmitters for this task, by learning feature representations using a deep neural network that uses the I/Q data from received signals as input. After detection and elimination of the adversarial transmitters RFAL further uses this learned feature embedding as “fingerprints” for categorizing the trusted transmitters. More specifically, we implement a generative model that learns the sample space of the I/Q values of known transmitters and uses the learned representation to generate signals that imitate the transmissions of these transmitters. We program 8 universal software radio peripheral (USRP) software defined radios (SDRs) as trusted transmitters and collect “over-the-air” raw I/Q data from them using a Realtek Software Defined Radio (RTL-SDR), in a laboratory setting. We also implement a discriminator model that discriminates between the trusted transmitters and the counterfeit ones with 99.9% accuracy and is trained in the GAN framework using data from the generator. Finally, after elimination of the adversarial transmitters, the trusted transmitters are classified using a convolutional neural network (CNN), a fully connected deep neural network (DNN) and a recurrent neural network (RNN) to demonstrate building of an end-to-end robust transmitter identification system with RFAL. Experimental results reveal that the CNN, DNN, and RNN are able to correctly distinguish between the 8 trusted transmitters with 81.6%, 94.6% and 97% accuracy respectively. We also show that better “trusted transmission” classification accuracy is achieved for all three types of neural networks when data from two different types of transmitters (different manufacturers) are used rather than when using the same type of transmitter (same manufacturer).